

ORIGINAL

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

- - - - -X

UNITED STATES OF AMERICA

:

SEALED  
INDICTMENT

- v. -

:

12 CRIM 185

RYAN ACKROYD,

:

a/k/a "kayla,"

:

a/k/a "lol,"

a/k/a "lolspoon,"

JAKE DAVIS,

:

a/k/a "topiary,"

:

a/k/a "atopiary"

DARREN MARTYN,

:

a/k/a "pwnsauce,"

a/k/a "raepsauce,"

a/k/a "networkkitten," and

DONNCHA O'CEARRBHAIL,

:

a/k/a "palladium,"

Defendants.

:

USDC SDNY  
DOCUMENT  
ELECTRONICALLY FILED  
DOC #:  
DATE FILED: 2/27/12

- - - - -X

COUNT ONE

(CONSPIRACY TO COMMIT COMPUTER HACKING - INTERNET FEDS)

The Grand Jury charges:

BACKGROUND ON ANONYMOUS AND INTERNET FEDS

1. Since at least in or about 2008, up through and including on or about the date of this Indictment, "Anonymous" has been a loose confederation of computer hackers and others sharing, among other things, common interests, common slogans, and common identifying symbols. During that time period, certain members of Anonymous have waged a deliberate campaign of online destruction, intimidation, and criminality, as part of which they have carried out cyber attacks against businesses and

government entities in the United States and throughout the world.

2. Between in or about December 2010 and in or about May 2011, one group of individuals affiliated with Anonymous who engaged in such criminal conduct was composed of elite computer hackers who collectively referred to themselves as "Internet Feds." At various times relevant to this Indictment, members of Internet Feds carried out a series of cyber attacks against the websites and computer systems of certain business and government entities in the United States and around the world, including, among others, the following businesses and organizations:

a. Fine Gael, a political party in Ireland, which maintained the website "www.finegael2011.com;"

b. HBGary, Inc. and its affiliate, HBGary Federal, LLC (collectively referred to herein as "HBGary"), computer security firms based in the United States which provided computer security software and services, among other things, to their clients, and which maintained the website "www.HBGaryFederal.com;" and

c. Fox Broadcasting Company ("Fox"), a commercial broadcast television network in the United States, which maintained the website "www.fox.com."

3. These cyber attacks involved, among other things: (1) breaking into computer systems, deleting data, and stealing

confidential information, including encrypted and unencrypted sensitive personal information for thousands of individual victims; (2) de-encrypting confidential information stolen from victims' computer systems, including encrypted passwords; (3) publicly disclosing that stolen confidential information on the Internet by dumping it on certain websites; (4) hijacking victims' email and Twitter accounts; (5) defacing victims' Internet websites; and/or (6) "doxing," that is, publicly disclosing online a victim's personal identifying information, such as the victim's name, address, Social Security number, email account, and telephone number, with the object of, among other things, intimidating the victim and subjecting the victim to harassment.

4. At various times relevant to this Indictment, and as part of Anonymous, members of Internet Feds sought to publicize their Internet assaults and intimidate their victims by, among other things: (1) posting messages online in which they discussed their attacks and threatened additional attacks; (2) using particular logos and slogans when, for example, they posted messages online and defaced websites; and (3) discussing their attacks with members of the press.

5. At various times relevant to this Indictment, and much like other members of Anonymous, members of Internet Feds, despite their efforts to publicize their illegal conduct,

typically attempted to hide their true identities by, for example, using aliases when they communicated with the public or with each other.

6. At various times relevant to this Indictment, members of Internet Feds, much like other members of Anonymous, communicated using, among other means, Internet Relay Chat ("IRC") channels -- that is, real-time, text-based online forums. Some of these channels were open to the public. Others, particularly channels in which members of Anonymous and members of Internet Feds planned and organized criminal activity, including cyber attacks, were not. Instead, those channels were generally password-restricted and available by invitation only, usually to trusted individuals who had proven themselves through past criminal hacking. Specifically, members of Internet Feds and their co-conspirators planned and coordinated their cyber attacks using password-restricted, invitation-only IRC channels such as "#InternetFeds," "#Hackers," and "#hq," among others.

7. At various times relevant to this Indictment, the members of Internet Feds included, among others, RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," and DONNCHA O'CEARRBHAIL, a/k/a "palladium," the defendants, as well as

other individuals, including, but not limited to, individuals who used the online aliases "SABU," "TFLOW," and "AVUNIT."

THE DEFENDANTS

8. At all times relevant to this Indictment, RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," and JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," the defendants, were computer hackers who resided in the United Kingdom.

9. The role of RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," the defendant, in each of the conspiracies charged in this Indictment included, among other things, identifying and exploiting vulnerabilities in victims' computer systems for the purpose of gaining unauthorized access to those systems.

10. The role of JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," the defendant, in each of the conspiracies charged in this Indictment included, among other things, acting as a spokesman for the groups charged in Counts One and Two of this Indictment, for example by engaging in interviews with the media and publicizing those groups' hacking activities; and organizing and storing confidential information stolen in connection with the computer hacking described in Counts One and Two of this Indictment.

11. At all times relevant to this Indictment, DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a

"networkkitten," and DONNCHA O'CEARRBHAIL, a/k/a "palladium," the defendants, were computer hackers who resided in Ireland.

CYBER ATTACKS BY INTERNET FEDS

12. From in or about December 2010, up to and including in or about May 2011, members of Internet Feds, including RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," and DONNCHA O'CEARRBHAIL, a/k/a "palladium," the defendants, and their co-conspirators, including, among others, SABU, TFLOW and AVUNIT, launched cyber attacks on, and gained unauthorized access to, the websites and computers systems of the following victims, among others:

Hack of Fine Gael

a. In or about January 2011, MARTYN and O'CEARRBHAIL participated in a cyber attack on Fine Gael's website, [www.finegael2011.com](http://www.finegael2011.com). Among other things, MARTYN and O'CEARRBHAIL accessed without authorization computer servers in Arizona used by Fine Gael to maintain its website, and uploaded code that defaced the website.

Hack of HBGary

b. In or about February 2011, ACKROYD, DAVIS, MARTYN, and their co-conspirators, including SABU, TFLOW and

AVUNIT, participated in a cyber attack on the website and computer systems of HBGary.

c. Among other things, ACKROYD, DAVIS, MARTYN, and their co-conspirators accessed without authorization computer servers used by HBGary in California and Colorado and stole confidential information from those servers, including approximately 60,000 emails from email accounts used by HBGary employees and a senior executive of HBGary Federal, LLC (the "HBGary Federal Executive"), which ACKROYD, DAVIS, and MARTYN, and their co-conspirators publicly disclosed via the [www.thepiratebay.org](http://www.thepiratebay.org) website (an anonymous file sharing website that permits users to post stolen content), among other means.

d. ACKROYD, DAVIS, MARTYN, and their co-conspirators used information gained from those stolen emails to access, without authorization, and steal the contents of an email account belonging to a senior executive of HBGary, Inc. (the "HBGary, Inc. Executive"); gain unauthorized access to the servers for the website [www.rootkit.com](http://www.rootkit.com), an online forum on computer hacking maintained by the HBGary, Inc. Executive, and steal confidential data, including usernames and encrypted passwords for approximately 80,000 user accounts; access without authorization and deface the Twitter account of the HBGary Federal Executive; and dox the HBGary Federal Executive by, among other things, posting his Social Security number and home

address on his Twitter account without his authorization or approval.

e. ACKROYD, DAVIS, MARTYN, and their co-conspirators de-encrypted tens of thousands of the encrypted www.rootkit.com users' passwords that they had stolen, and publicly disclosed those de-encrypted passwords, the rootkit.com usernames they had stolen, and the contents of the email account belonging to the HBGary, Inc. Executive, by dumping them on certain Internet websites.

Hack of Fox

f. In or about April 2011, ACKROYD, DAVIS, MARTYN, O'CEARRBHAIL, and their co-conspirators, including SABU, TFLOW and AVUNIT, participated in a cyber attack on the website and computer systems of Fox.

g. Among other things, ACKROYD, DAVIS, MARTYN, O'CEARRBHAIL, and their co-conspirators accessed without authorization computer servers in California used by Fox and stole and publicly disclosed confidential information, including a database of the names, dates of birth, telephone numbers, email addresses, and residences, among other information, for more than 70,000 potential contestants on "X-Factor," a Fox television show.



STATUTORY ALLEGATIONS

13. From at least in or about December 2010, up to and including in or about May 2011, in the Southern District of New York and elsewhere, RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," and DONNCHA O'CEARRBHAIL, a/k/a "palladium," the defendants, and others known and unknown, willfully and knowingly, combined, conspired, confederated, and agreed together and with each other to engage in computer hacking, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

14. It was a part and an object of the conspiracy that RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," and DONNCHA O'CEARRBHAIL, a/k/a "palladium," the defendants, and others known and unknown, willfully and knowingly would and did cause the transmission of a program, information, code and command, and, as a result of such conduct, would and did intentionally cause damage without authorization, to a protected computer, which would and did cause a loss (including loss resulting from a related course of conduct affecting one and more other protected computers) aggregating to at least \$5,000

to one and more persons during any one year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i) and (c)(4)(A)(i)(I).

OVERT ACTS

15. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about January 9, 2011, DONNCHA O'CEARRBHAIL, a/k/a "palladium," the defendant, sent an electronic communication to DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," the defendant, containing computer code to be used to deface the www.finegael2011.com website.

b. In or about February 2011, SABU used a computer located in New York, New York to access without authorization computer servers used by HBGary and steal tens of thousands of emails belonging to employees of HBGary and the HBGary Federal Executive.

c. In or about February 2011, JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," the defendant, accessed without authorization the Twitter account of the HBGary Federal Executive and posted one or more fraudulent tweets.

d. In or about February 2011, RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," the defendant, accessed without authorization an email account belonging to the HBGary, Inc. Executive and sent one or more fraudulent emails from that account to an administrator for the [www.rootkit.com](http://www.rootkit.com) website requesting administrative access to that website.

e. On or about February 7, 2011, TFLOW uploaded links to tens of thousands of stolen emails belonging to employees of HBGary and the HBGary Federal Executive as well as a copy of certain text that had been used to deface the [www.HBGaryFederal.com](http://www.HBGaryFederal.com) website, to an account on the website [www.thepiratebay.org](http://www.thepiratebay.org) in the name "HBGary leaked emails."

f. On or about February 8, 2011, DAVIS, using the IRC channel #hq, discussed how Twitter had locked the Twitter account of the HBGary Federal Executive and stated, "That works in our favour. His Twitter still has all our tweets. Including his SSN."

g. On or about February 9, 2011, ACKROYD, using the IRC channel #hq, asked TFLOW whether he had received a copy of emails belonging to the HBGary, Inc. Executive, to which TFLOW responded affirmatively and stated that he would add them to an "online viewer."

h. On or about February 12, 2011, SABU, using the IRC channel #hq, stated that he had deleted data on a server used by HBGary.

i. On or about February 13, 2011, DAVIS, using the IRC channel #hq, told AVUNIT "I'm happy to talk to press on IRC/Skype, have done [so] for months," and told TFLOW that he had "talked to maybe 150 journalists."

j. In or about May 2011, SABU used a computer in New York, New York to access without authorization a computer server used by Fox and download a database containing personal information relating to potential contestants on the X-Factor television show.

(Title 18, United States Code, Section 1030(b).)

COUNT TWO

(CONSPIRACY TO COMMIT COMPUTER HACKING - LULZSEC)

The Grand Jury further charges:

16. The allegations in paragraphs 1 through 12 and 15 this Indictment are repeated and realleged as though fully set forth herein.

BACKGROUND ON LULZSEC

17. In or about May 2011, following the publicity that they had generated as a result of their hacking of Fine Gael and HBGary, among other victims, members of Internet Feds, including RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a

"lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," and DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," the defendants, as well as SABU, TFLOW, and AVUNIT, formed and became the principal members of a new hacking group, "Lulz Security" or "LulzSec."

18. Like Internet Feds, LulzSec undertook a campaign of malicious cyber assaults on the websites and computer systems of various business and government entities in the United States and throughout the world. Although the members of LulzSec and their co-conspirators claimed to have engaged in these attacks for humorous purposes ("lulz" is Internet slang which can be interpreted as "laughs," "humor," or "amusement"), LulzSec's criminal acts included, among other things, the theft of confidential information, including sensitive personal information for thousands of individuals, from their victims' computer systems; the public disclosure of that confidential information on the Internet; the defacement of Internet websites; and overwhelming victims' computers with bogus requests for information (known as "denial of service" or "DoS" attacks).

19. Also like Internet Feds, LulzSec sought to gain notoriety for their hacks by varied and repeated efforts to broadcast their acts of online destruction and criminality. As a means of publicizing their cyber assaults, members of LulzSec

and their co-conspirators maintained a website, "www.LulzSecurity.com;" an account in the name "LulzSec" at www.thepiratebay.org; and a Twitter account, "@LulzSec;" all of which they used to, among other things, announce their hacks and issue written "press releases" about them; mock their victims; solicit donations; and publicly disclose confidential information they had stolen through their cyber attacks.

20. Similar to Internet Feds, as a means of publicizing their online assaults, as well as intimidating their victims, members of LulzSec and their co-conspirators used particular logos and slogans in, for example, their "press releases," their website defacements, and on the www.LulzSecurity.com website and the @LulzSec Twitter account.

21. Despite going to great lengths to seek attention for their illegal conduct, the members of LulzSec and their co-conspirators - like Internet Feds - attempted to hide their true identities. Among other things, they referred to themselves by aliases, attempted to promote false personas, and used technical means, including proxy servers, in an effort to conceal themselves online.

22. At various times relevant to this Indictment, members of LulzSec, including RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," and DARREN MARTYN, a/k/a "pwnsauce," a/k/a

"raepsauce," a/k/a "networkkitten," the defendants, as well as SABU, TFLOW, and AVUNIT, and their co-conspirators, launched cyber attacks on the websites and computer systems of the following victims, among others:

a. Sony Pictures Entertainment ("Sony Pictures"), a division of Sony, a global electronics and media company, which produced and distributed television shows and movies and maintained the website "www.sonypictures.com;"

b. The Public Broadcasting Service ("PBS"), a non-profit public television broadcasting service in the United States, which maintained the website "www.pbs.org;"

c. The Atlanta, Georgia chapter of the Infragard Members Alliance ("Infragard-Atlanta"), an information sharing partnership between the Federal Bureau of Investigation ("FBI") and private industry concerned with protecting critical infrastructure in the United States, which maintained the website "www.infraguardatlanta.org;" and

d. Bethesda Softworks, a video game company based in Maryland, which owned the videogame "Brink" and maintained the website "www.brinkthegame.com."

23. At various times relevant to this Indictment, and in addition to identifying and exploiting vulnerabilities in their victims' computer systems on their own, the members of LulzSec also received from other computer hackers information

regarding vulnerabilities in the computer systems of a variety of business and government entities. LulzSec members used this information to launch cyber attacks on those entities or stored it in anticipation of future attacks.

24. At various times relevant to this Indictment, members of LulzSec and their co-conspirators communicated with each other and planned and coordinated their cyber attacks using password-restricted, invitation-only IRC channels, including, among others, "#upperdeck" and "#hq".

CYBER ATTACKS BY LULZSEC

25. From in or about May 2011, up to and including at least in or about June 2011, members of LulzSec, including RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," and DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," the defendants, and their co-conspirators, including, among others, SABU, TFLOW, and AVUNIT, launched cyber attacks on, and gained unauthorized access to, the websites and computers systems of the following victims, among others:

Hack of PBS

a. In or about May 2011, ACKROYD, DAVIS, MARTYN, and their co-conspirators, including SABU, TFLOW and AVUNIT, in retaliation for what they perceived to be unfavorable news coverage in an episode of the PBS news program Frontline,



undertook a cyber attack on the website and computer systems of PBS.

b. ACKROYD, DAVIS, MARTYN, and their co-conspirators, accessed without authorization computer servers in Virginia used by PBS, stole confidential information from those servers, including, among other things, databases containing names, email addresses, usernames and passwords of more than approximately 2,000 PBS employees and other individuals and entities associated with PBS; publicly disclosed that information on certain websites, including the [www.LulzSecurity.com](http://www.LulzSecurity.com) website; and defaced the PBS website, including by inserting a bogus news article.

Hack of Sony Pictures

c. In or about May 2011, ACKROYD, DAVIS, and their co-conspirators, including SABU, TFLOW and AVUNIT, participated in a cyber attack on computer systems used by Sony Pictures. This attack included accessing without authorization Sony Pictures' computer servers in California, and stealing and publicly disclosing on certain websites, including the [www.LulzSecurity.com](http://www.LulzSecurity.com) website, confidential information for at least approximately 100,000 users of the [www.sonypictures.com](http://www.sonypictures.com) website, including the users' passwords, email addresses, home addresses, and dates of birth.

Hack of Infragard-Atlanta

d. In or about June 2011, ACKROYD, DAVIS, MARTYN, and their co-conspirators, including SABU, TFLOW and AVUNIT, launched cyber attacks on the website and computer systems of Infragard-Atlanta. These attacks included stealing the login credentials, encrypted passwords, and other confidential information for approximately 180 users of the Infragard-Atlanta website, [www.atlantainfraguard.org](http://www.atlantainfraguard.org); defacing that website; de-encrypting the stolen passwords; and publicly disclosing the stolen confidential user information, including the de-encrypted passwords, on certain websites, including the [www.LulzSecurity.com](http://www.LulzSecurity.com) website.

Hack of Bethesda Softworks

e. In or about June 2011, ACKROYD, DAVIS, MARTYN, and their co-conspirators, including TFLOW, participated in a cyber attack on the computer systems used by Bethesda Softworks, stealing confidential information, including authorization keys, as well as usernames, passwords, and email accounts for approximately 200,000 users of Bethesda Softworks' website, "[www.brinkthegame.com](http://www.brinkthegame.com)." ACKROYD, DAVIS, MARTIN, and their co-conspirators, publicly disclosed some of that stolen data on certain websites, including the [www.LulzSecurity.com](http://www.LulzSecurity.com) website.

STATUTORY ALLEGATIONS

26. From at least in or about May 2011, up to and including at least in or about June 2011, in the Southern District of New York and elsewhere, RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," and DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," the defendants, and others known and unknown, willfully and knowingly, combined, conspired, confederated, and agreed together and with each other to engage in computer hacking, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

27. It was a part and an object of the conspiracy that RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," and DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," the defendants, and others known and unknown, willfully and knowingly would and did cause the transmission of a program, information, code and command, and, as a result of such conduct, would and did intentionally cause damage without authorization, to a protected computer, which would and did cause a loss (including loss resulting from a related course of conduct affecting one and more other protected computers) aggregating to at least \$5,000 to one and more persons during any one year period, and which would and did cause damage

affecting a computer used by and for an entity of the United States Government, to wit the FBI, in furtherance of the administration of justice, national defense and national security, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i) and (c)(4)(A)(i)(I) and (V).

OVERT ACTS

28. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about May 6, 2011, JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," the defendant, established a Twitter account in the name "@LulzSec."

b. In or about May 2011, SABU used a computer located in New York, New York, to gain unauthorized access to computer systems used by PBS and install one or more surreptitious means ("backdoors") by which SABU and others could secretly re-access those systems without authorization.

c. In or about May 2011, DAVIS wrote a bogus news article, which was used to deface the www.pbs.org website.

d. In or about May 2011, RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," the defendant, and SABU accessed without authorization computer servers used by PBS and downloaded confidential information.

e. In or about May 2011, SABU used a computer located in New York, New York, to gain unauthorized access to servers used by Sony Pictures.

f. In or about June 2011, SABU used a computer located in New York, New York to gain unauthorized access to, and install one or more backdoors in, computer systems used by Infragard-Atlanta.

g. In or about June 2011, ACKROYD accessed without authorization servers used by Infraguard-Atlanta and downloaded confidential information.

h. In or about June 2011, a co-conspirator not named as a defendant herein provided information concerning a vulnerability in computer systems used by Bethesda Softworks to ACKROYD and other members of LulzSec.

i. On or about June 12, 2011, ACKROYD used the foregoing vulnerability to gain unauthorized access to computer systems used by Bethesda Softworks, install one or more backdoors, which he provided to other members of LulzSec, and download confidential information.

j. In or about June 2011, DAVIS used a backdoor provided by ACKROYD to access without authorization computer systems used by Bethesda Softworks and download confidential information, which DAVIS then organized.

k. On or about June 12, 2011, MARTYN posted the following message in the IRC channel #upperdeck: "Ok, who are we raping, brink?" to which ACKROYD responded affirmatively.

l. On or about June 12, 2011, DAVIS posted the following message in the IRC channel #upperdeck: "so everyone knows, Brink leakage is 100% organized on my end; just waiting on the 200K DB."

m. On or about June 21, 2011, a co-conspirator not named as a defendant herein provided SABU with confidential files relating to a computer network at the "madison ave hq in nyc" of Sony Music Entertainment, a division of Sony.

(Title 18, United States Code, Section 1030(b).)

FORFEITURE ALLEGATION AS TO COUNTS ONE AND TWO

29. As a result of committing one or both of the offenses alleged in Counts One and Two of this Indictment, RYAN ACKROYD, a/k/a "kayla," a/k/a "lol," a/k/a "lolspoon," JAKE DAVIS, a/k/a "topiary," a/k/a "atopiary," DARREN MARTYN, a/k/a "pwnsauce," a/k/a "raepsauce," a/k/a "networkkitten," and DONNCHA O'CEARRBHAIL, a/k/a "palladium," the defendants, shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(2)(B), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of one or both of the said offenses, including but not limited to a sum of

money representing the amount of proceeds obtained as a result of one or both of the said offenses.

SUBSTITUTE ASSETS PROVISION

30. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third person;

c. has been placed beyond the jurisdiction of the Court;

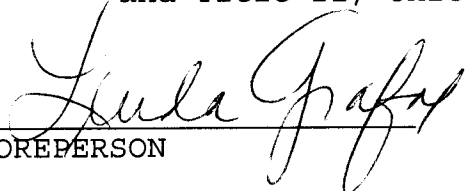
d. has been substantially diminished in value;  
or

e. has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to 18 U.S.C.

§ 982(b)(1) and 21 U.S.C. § 853(p), to seek forfeiture of any other property of said defendants up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 982(a)(2)(B) and (b)(1), and Title 21, United States Code, Section 853(p).)

  
FOREPERSON

  
PREET BHARARA  
United States Attorney



Form No. USA-33s-274 (Ed. 9-25-58)

---

---

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

---

---

UNITED STATES OF AMERICA

- v. -

RYAN ACKROYD,  
a/k/a "kayla,"  
a/k/a "lol,"  
a/k/a "lolspoon,"  
JAKE DAVIS,  
a/k/a "topiary,"  
a/k/a "atopiary"  
DARREN MARTYN,  
a/k/a "pwnsauce,"  
a/k/a "raepsauce,"  
a/k/a "networkkitten," and  
DONNCHA O'CEARRBHAIL,  
a/k/a "palladium,"

Defendants.

---

---

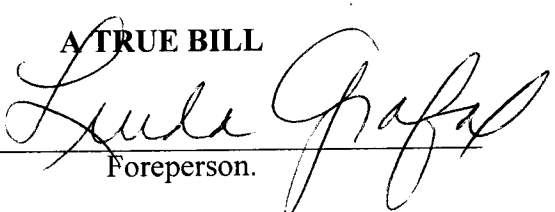
INDICTMENT

12 Cr. \_\_\_\_\_

18 U.S.C. § 1030(b).

PREET BHARARA  
United States Attorney.

A TRUE BILL

  
Foreperson.

*SUPERSEDEDING*

*2/27/12 - Filed Sealed Indictment. Arrest warrants issued.*

*J. KATZ  
U.S.M.S.*